THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF SOUTH CAROLINA
CHARLESTON DIVISION

IN THE MATTER OF THE SEARCH OF ELECTRONIC DEVICES DESCRIBED IN ATTACHMENT A TO THE AFFIDAVIT OF SPECIAL AGENT MICHAEL STROBL DATED MARCH 8, 2022	Case No.: 2:22-cr-571

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Special Agent Michael Strobl, your Affiant, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent of the United States Secret Service (USSS) and have been so employed since November 2007. As a Special Agent of the United States Secret Service, I received extensive training at the Federal Law Enforcement Training Center and the James J. Rowley Training Center. This training covered all aspects of financial investigations including credit card fraud and identity theft, and I have participated in numerous investigations of violations of criminal law including matters involving fraud and white-collar crime.

2. I am currently assigned to the Charleston, South Carolina USSS Resident Office. I have received training from several agencies, including the USSS, into cell phone and computer analysis. This includes training in investigating technological devices, electronic accounts, and ways in which criminals use electronic communications (e.g., e- mail,

social media, and online communications platforms) to further criminal activity. Through my training, education, and experience, I have become familiar with the manner in which criminals communicate and operate their clandestine activities, including through Internet marketplaces and e-mail accounts.

3. I have participated in investigations of state and federal offenses to include, counterfeit currency, wire fraud, bank fraud, identity theft and other financial related crimes. Accordingly, I am thoroughly familiar with the investigative techniques used in these investigations, such as the use of cooperating witnesses and confidential informants, surveillance, search and seizure warrants, and the interception of communications. In addition, based on my experience, I know that individuals engaged in financial related crimes often maintain evidence on personal communication platforms, including e-mail accounts. This is particularly true where those individuals use the internet to facilitate and further their criminal conduct.

4. I have personal knowledge or have been provided by other law enforcement officers with the facts set forth herein. Since this affidavit is being submitted for the limited purpose of obtaining a search warrant, I have not included every fact known to me concerning this investigation; rather, I have set forth only the facts necessary to establish probable cause.

5. Based on my training and experience and the facts set forth in this affidavit, there is probable cause to believe that violations of Title 18, United States Code, Sections 1343 and 1029(a)(2) have been committed and that evidence exists on the electronic devices described in Attachment A. There is probable cause to search the electronic devices described in Attachment A for evidence of these crimes, as described in Attachment B.

IDENTIFICATION OF THE DEVICES TO BE EXAMINED

6. This affidavit is submitted in support of an application to search the following electronic devices, which are described in Attachment A:

a. An Acer Laptop (Serial Number LXRDR020381301B8B21601) along with any removable media.

b. An HP Laptop (Serial Number 3T894703D0) along with any removable media.

c. An HP Laptop (Model Chromebook, Serial Number 5CD822BWB2) along with any removable media.

d. A Samsung Cellular Phone (SM-J700T1, Serial Number J700T1UVU2APK6) along with its contained SIM card and any removable media.

e. An BLU Cellular Phone (Serial Number 1070339021027808) along with its contained SIM card and any removable media.

f. A Cruzer Digital Storage Device (Model Glide Cruzer 128 GB Thumbdrive).

g. A Cruzer Digital Storage Device (Model Glide Cruzer 64 GB Thumbdrive).

7. The applied-for warrant would authorize the forensic examination of the Devices for the purpose of identifying electronically stored data particularly described in Attachment B.

STATEMENT OF PROBABLE CAUSE

8. In August 2021, USSS SSA Iris Jolliff and TFO James "Gil" Jackson with the City of Charleston Police Department ("CPD") met with Lowe's Home Improvement Organized Crime Retail Manager Andria Hall ("Hall").

9. Hall presented SSA Jolliff and TFO Jackson with a Lowe's investigation into **CALEB HOOD ("HOOD").** Lowe's internal investigation has revealed that **HOOD** was stealing merchandise from Lowe's retail locations with the District of South Carolina and then returning it

to a different Lowe's retail location in the District of South Carolina for a refund in the form of a merchandise card.

10. Specifically, **HOOD** was stealing from Lowe's and perpetrating his scheme in Charleston County.

11. The USSS began its own investigation into the activities of **HOOD**, and the following was discovered:

a. **HOOD** was working under the false identities of James Woodbury and/or Anthony Tisdale.

b. **HOOD** would enter a Lowe's retail location in the District of South Carolina, and elsewhere, with merchandise he had previously stolen from a different Lowe's retail location.

c. **HOOD** would present himself to the return desk and claim he did not have the receipts for the merchandise he sought to return. This would generate a merchandise card from Lowe's. The amount issued on each merchandise card of the returned merchandise would range from $100-200.

d. **HOOD** has been operating this scheme since April 2018 and your affiant believes he was operating it up to the date of his arrest of March 2, 2022.

e. As of January 26, 2022, the current loss amount to Lowe's is approximately $147,000.

12. As set forth above, **HOOD** is believed to have begun this scheme in April 2018 and has continued it to as recently as February 12, 2022. In discussions with Hall, she advised HOOD conducted fraudulent returns of items not purchased on January 29th and 30th. **HOOD** also conducted fraudulent returns of items not purchased on February 1st, February 5th through 8th,

February 11th, and February 12th.

13. In fact, while conducting a post Miranda interview on March 2, 2022, **HOOD** admitted that he was on his way to commit the same acts when he was arrested.

14. Throughout your Affiant's investigation, it has been determined that Lowe's policy for issuing refunds on items that were returned without a receipt required the customer to submit a driver's license or other government-issued identification to receive a merchandise card, similar to a gift card, in the amount of the refund. The merchandise card could be used to purchase merchandise at any Lowe's retail store.

15. It is common knowledge, computers can be used to access the internet for the purpose of researching business locations, addresses and hours of operation. They also contain storage and word processing capability to produce documents and images. Computers can also be utilized to access business webpages and make purchases using fraudulently obtained merchandise cards. In addition, and based on my investigative experience, subjects will commonly use computers to assist them in making or purchasing fraudulent identifications and similar paperwork. Most individuals today possess a cellular telephone which are able to perform a multitude of function, including but not limited to, making phone calls, sending text message, email, internet access and Global Positioning System (GPS). They also contain application used to assist in directions from place to place. Modern cellular phones possess current and historical GPS location data that can closely pinpoint the exact location fo the phone. Based on my investigative experience, subjects will utilize their cellular telephones to communicate with co-conspirators via phone, text and/or email. They will also use the phone's internet ability to research business addresses and hours as well as utilize the GPS to get turn by turn directions to the business they intend to defraud.

16. Throughout your Affiant's investigation, your Affiant has conducted an inquiry to determine that it was **HOOD** who was operating under the identities of James Woodbury and/or Anthony Tisdale. The following has been determined:

a. When Lowe's began to notice the frequency of the returns by James Woodbury and/or Anthony Tisdale, it began to research the returns. In its research, one merchandise card was tracked that included a partial purchase with a debit card belonging to "Caleb Taekwon Hood".

b. Lowe's cross-referenced **HOOD**'s photographs with photographs and video of returns made by James Woodbury and/or Anthony Tisdale and determined that it was in fact **HOOD** operating under these identities.

c. Further supporting the determination that it was **HOOD**, is a citation issued to **HOOD** by the Belmont, NC police department in October 2021.

d. In October 2021, the Belmont, NC Police Department (BPD) was called to a Lowe's retail location due to suspicious activity. When Officer Tucker (BPD) arrived at the Lowe's, he encountered **HOOD**. During the conversation with **HOOD**, the following were obtained from **HOOD**'s person: **HOOD**'s South Carolina Driver's License and three (3) other Pennsylvania Driver's Licenses under the name James Woodbury. The picture on the Pennsylvania Driver's License was of **HOOD** but had none of his personal information. Two of the fraudulent Pennsylvania Driver's Licenses were located in plain view in the vehicle that **HOOD** was driving when this incident occurred. The vehicle **HOOD** was driving at the time of this incident was a white Chevy Malibu Sedan. Officer Tucker (BPD)

identified the vehicle as belonging to Ashley Black.

e. Your Affiant has determined that **HOOD** has an outstanding warrant that is still active with the Belmont, NC Police Department for "obtaining property by false pretenses".

17. Your Affiant has determined through the investigation that once **HOOD** was cited by BPD for using the false identity of James Woodbury, in December 2021, **HOOD** began using a Driver's License from the State of Massachusetts under the name Anthony Tisdale.

18. Your Affiant presented the facts of USSS's investigation to AUSA Amy Bower in January 2022. An indictment was presented to a Federal Grand Jury on February 8, 2022, and a four-count indictment was true billed.

19. **HOOD** has been indicted on three counts of violation of 18 U.S.C. §1343, wire fraud, and one count of access device fraud under 18 U.S.C. §1029(a)(2).

20. On February 28, 2022, a search warrant package was presented to the Honorable Mary Gordon Baker to search **HOOD**'s residence identified on his SCDMB record, 1521 Saint Anthony Ave., Apt A, Florence, SC 29505.

21. During the execution of the warrant of **HOOD'**s residence located at 1521 Saint Anthony Ave., Apt. A, Florence, SC 29505 ("St. Anthony's Residence"), other forms of identification were recovered that have photographs of persons who are not **HOOD**.

22. During the execution of the warrant at the St. Anthony's Residence, it was discovered that **HOOD** also rents a second apartment located at **513 Coit Street, Apt. B, Florence, SC 29501** ("Coit Residence"). A search warrant package was presented to the Honorable Molly H. Cherry on March 2, 2022 to search **HOOD**'s premise located at **513 Coit Street, Apt. B, Florence, SC 29501**.

23. In the execution of the federal search warrant at the St. Anthony's Residence, **HOOD** was interviewed. During the interview, **HOOD** made statements that he separates and conceals his criminal activity from Ashley Black and her children whom reside with **HOOD** at the St. Anthony's residence. **HOOD** also stated that he manufactures the fraudulent driver's licenses on computers and prints the Driver's Licenses himself.

24. On March 2, 2022, USSS executed the search warrant for **HOOD**'s Coit Residence. Agents seized numerous pieces of evidence, including the electronic devices described in Attachment A (collectively referred to herein as "Devices"). All Devices were seized by USSS and are currently in the lawful possession of USSS Charleston. The Devices were seized pursuant to the search warrant signed by the Honorable Molly H. Cherry. Attachment B to the search warrant required the undersigned apply to this Court for a subsequent warrant to examine the Devices.

25. I know that cellular telephones, storage mediums, and computers are often used by individuals to facilitate the commission of criminal acts, including the crime of identity theft and wire fraud. Further, I am aware that incriminating evidence is often located within text messages, as well as photos and videos contained on cellular telephones. Additionally, call logs (for incoming, outgoing, and missed calls), stored contact lists, and location information have proven to be valuable evidence in criminal cases. Moreover, I am familiar with technology that allows law enforcement investigators to harvest data (such as incoming and outgoing text messages, photos, videos, call logs, and contacts) from cellular telephones. I also know that it is common for individuals involved in criminal activity to use cell phones subscribed in a name other than their own, and to use "pre-paid" cellular telephones for which no real subscriber information is available.

26. Additionally, based on my training and experience and the investigation thus far, I believe **HOOD** uses his personal cell phone to facilitate the fraud, including but not limited through phone calls, text messages, and e-mails. In addition, during a post Miranda Interview with **HOOD**, he admitted to manufacturing the fraudulent driver's licenses accessing website and application data via his digital devices. **HOOD** also admitted to using social media (Facebook) to communicate with individuals who were a part of the scheme. Based on the patterns uncovered in this investigation, as further described below, I respectfully submit there is probable cause to believe that **HOOD** uses his personal cell phone and computers to perpetuate the fraud described herein, and that now concealed on that device is evidence of the criminal violations described in this affidavit.

27. Further based on my training and experience and the investigation thus far, I believe **HOOD** used his personal laptop computers and storage mediums to access the program to manufacture the fraudulent identifications from various states. During a post Miranda interview with **HOOD**, he admitted to manufacturing the fraudulent driver's licenses using his computers and printers. **HOOD** would have had to access the websites via a browser that will contain the date and time of the websites she visited.

28. The Devices are currently in storage at 1671 Belle Isle Ave., Suite 225, Mt. Pleasant, SC 29464. In my training and experience, I know that the Devices have been stored in a way in which their contents are, to the extent material to this investigation, in substantially the same state as they were when the Devices first came into the possession of USSS.

TECHNICAL TERMS

107 Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Computer: a computer includes all types of electronic, magnetic, optical, electrochemical, or other high-speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

b. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining

the location of the device.

c. Storage medium: a storage medium includes any physical object upon which computer data can be recorded, including external and internal hard drives, flash drives, thumb drives, micro-SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact discs, magnetic tapes, memory cards, memory chips, and other magnetic or optical media.

d. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

e. Portable media player: A portable media player (or "MP3 Player" or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable

media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

f. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

g. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for

entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device.

h. IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

i. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

108 Based on my training, knowledge and experience, and the experience of others with whom I have discussed this investigation, I know that the Devices have capabilities that allow

them to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, and PDA. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

109 Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

110 *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Devices were used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Devices because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to

draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

111 *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the Devices consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the Devices to human inspection in order to determine whether it is evidence described by the warrant.

112 *Manner of execution.* Because this warrant seeks only permission to examine devices already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

113 In my experience with investigations involving fraud similar to the type described herein, I believe there is probable cause to believe that evidence of **HOOD**'s violations of Title18 U.S.C. §1343 and §1029(a)(2) will be present on the computers, cell phones and other digital devices that were discovered at the Coit Residence. Often when committing crimes, targets keep multiple devices and store fruits and instrumentalities of the crimes in multiple devices. In other cases, similar to this one that I have personally investigated, multiple devices have been used to commit the fraudulent activity.

114 This affidavit has been reviewed by Assistant United States Attorney Amy Bower.

Respectfully submitted,

mstrobl Digitally signed by mstrobl
Date: 2022.03.08 10:47:34
-05'00'

Michael Strobl, Senior Special Agent
United States Secret Service

Sworn to me via telephone or other reliable electronic means and signed by me pursuant to Fed. R. Crim. P. 4.1 and 4(d) or 41(d)(3), as applicable on this the 8th day of March 2022.

UNITED STATES DISTRICT COURT
DISTRICT OF SOUTH CAROLINA

Molly H. Cherry

The Honorable Molly H. Cherry
United States Magistrate Judge